

UNITED STATES DISTRICT COURT

for the
Middle District of North Carolina ☒

In the Matter of the Search of

*(Briefly describe the property to be searched
or identify the person by name and address)*812 Northern Shores Point Greensboro, North Carolina,
27455 and the Person of David W. Schamens, Date of
Birth July 16, 1957

Case No. 21MJ323-1

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachments A-1 and A-2.

located in the Middle District of North Carolina, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. § 1343, 1344, 1956, 1957 and 15 U.S.C. §§ 78j(b) and 78ff	Wire fraud, Bank Fraud, Money Laundering, Transacting in Criminal Proceeds, and Securities Fraud.

The application is based on these facts:

See Attachment.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Attested to by the applicant in accordance with
the requirements of Fed. R. Crim. P. 4.1 by
telephone.

/s James Gallo

Applicant's signature

James Gallo, Special Agent, HSI

*Printed name and title*Date: 8/27/2021 8:48 a.m.City and state: Durham, North Carolina

Certified to be a true and
correct copy of the original.

John S. Brubaker, Clerk
U.S. District Court
Middle District of North Carolina

By: [Signature]
Deputy Clerk
Date: August 27, 2021

Judge's signature

Joe L. Webster, United States Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

In the Matter of the Search of
812 Northern Shores Point
Greensboro, North Carolina, 27455 and
the Person of David W. Schamens, Date
of Birth July 16, 1957

1:21MJ323-1

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, James Gallo, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent ("SA") with the Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations ("HSI"), and have been since November 2019. In 2020, I attended and successfully completed the Criminal Investigator Training Program (CITP) and the HSI Special Agent Training Program (HSISAT) at the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia. During which time I was specifically trained in criminal law and investigative procedures essential to the successful investigation, apprehension, and prosecution of criminal subjects. I also previously received additional training at FLETC specific to detecting and investigating violations of financial crimes. Prior to my tenure as a Special Agent, I was a duly sworn member of the New Jersey Division of Criminal Justice and had been since June 2014. There, I actively conducted numerous complex financial investigations. During the investigation of these cases, I participated in the execution of numerous arrests, search warrants, and seizures of evidence.

2. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search: (a) the following premises: 812 Northern Shores Point, Greensboro, North Carolina, 27455 (the "SUBJECT PREMISES"), as described in Attachment A-1; and (b) the person of David W. Schamens, date of birth July 16, 1957, as described in Attachment A-2.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts in this affidavit come from my personal observations, my training and experience, my review of documents, and information from other agents and witnesses.

4. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 1343 (wire fraud), 18 U.S.C. § 1344 (bank fraud), 18 U.S.C. § 1956 (money laundering), 18 U.S.C. § 1957 (transacting in criminal proceeds), and 15 U.S.C. §§ 78j(b) and 78ff, and 17 C.F.R. § 240.10b-5 (securities fraud) (the "Specified Federal Offenses") have been committed. There is also probable cause to search the SUBJECT PREMISES, described in Attachment A, for evidence and instrumentalities of the Specified Federal Offenses, as further described in Attachment B.

PROBABLE CAUSE

Overview

5. Since in or around January 2021, HIS has been investigating an investment fraud scheme being committed by David W. Schamens ("Schamens").

Schamens is the owner and operator of at least two proprietary trading groups called TD Trading LLC ("TD") and TFG Trading Fund LLC ("TFG") (the "Trading Groups"). Schamens operated the Trading Groups under the umbrella of another entity called Tradedesk Financial Group, Inc. ("Tradedesk"). Tradedesk, and the Trading Groups, purported to be customers of still another entity controlled by Schamens called TradeStream Analytics LTD ("TradeStream"). According to its website, TradeStream is a software-company, whose clients include paid subscribers who, for various legitimate reasons, needed direct access to trade-based services. Schamens is currently listed on the website as TradeStream's Chief Executive Officer.

6. Based on this investigation, from in or around 2014 through the present, Schamens used Tradedesk and the Trading Groups to fraudulently solicit funds from investors (the "Victim Investors"). Schamens falsely promised the Victim Investors that an investment in the Trading Groups would generate a monthly return on investment ("ROR") of 1% to 1.5% (12% to 18% annually). According to information Schamens provided to the Victim Investors, investments in the Trading Groups would be used to fund short-term investment loans made to day traders (the "Day Traders") who would conduct trading activity through TradeStream. Schamens further assured the Victim Investors that the Trading Groups' profits would be derived from fees imposed on the Day Traders and not the profitability of the trades made by the Day Traders through TradeStream. In reality, Schamens used the funds to: (a) finance his own lifestyle and make various personal expenditures; (b) pay back

prior Victim Investors in in the manner of a Ponzi scheme; and (c) make various expenditures unrelated to the investments made by the Victim Investors.

7. According to an investor presentation regarding TD (the “TD Investor Presentation”), which was provided to at least one of the Victim Investors:

- a. Cash deposits made by investors were SIPC insured on behalf of TD’s “clearing firm” and FDIC insured by the custodian bank;
- b. Cash deposits were “not at risk” because the funds would only provide buying power and were not going to be traded;
- c. The ROR on the cash deposits would be “based on trading volume and the routing fees that TradeStream charges and reimburses TD Trading, LLC for.” The TD Investor Presentation provided the following example: “a trader buys 1000 shares. TradeStream charges, depending on where executed, between \$.0010 and \$.0015 per share for routing. TradeStream shares this routing fee to TD Trading, LLC Class A members for use of capital by the Class B member traders¹ in generating trades.”;
- d. Investor funds could be withdrawn “without penalty” during the first 10 business days of the trading month and the funds were “always held as cash, not traded.”

Based on this investigation, Schamens made similar representations to Victim Investors about how TFG purported to operate.

8. Schamens accepted funds from the Victim Investors for investment in the Trading Groups primarily into one of three different bank accounts controlled by Schamens at Bank of America: (1) an account held in the name “TD Trading” ending in 6431 (“the TD BOA Account”); (2) an account held in the name “TFG Trading Fund”

¹ Class A members were the victim investors that were investing capital in one of the Trading Groups and Class B members traders were purportedly the Day Traders trading the capital through TradeStream.

ending in 9749 (the “TFG BOA Account”); and (3) an account held in the name “Tradedesk Financial Group” ending in 2714 (the “Tradedesk BOA Account”) (collectively, the “BOA Bank Accounts”).

9. Schamens received funds into the BOA Bank Accounts in one of two ways: (1) Victim Investors would wire or transfer funds directly to one or more of the BOA Bank Accounts; or (2) Victim Investors would transfer the balances of previously held Individual Retirement Accounts (“IRAs”) to one of two companies at Schamens’ direction: Millennium Trust Company (“Millennium”) and Mainstar Trust (“Mainstar”). At Schamens’ direction, the Victim Investors would then direct Millennium or Mainstar to invest the IRA funds with one of the Trading Groups and the funds would then be wired to one of the BOA Bank Accounts by Millennium or Mainstar. Based on this investigation, Schamens, at times, provided Millennium and Mainstar with fake records regarding the health of the Victim Investors’ investments with the Trading Groups to abate concerns raised by Millennium and Mainstar as custodians of the Victim Investors’ IRAs. The Victim Investors additionally made subsequent yearly contributions to the IRAs held at Millennium and Mainstar which were ultimately transferred to one of the BOA Accounts.

10. Schamens further took various steps to hide the fraudulent scheme from the Victim Investors and maintain their trust, including, but not limited to, by: (a) emailing the Victim Investors fabricated K-1 statements that falsely represented to the Victims Investors that their funds were secure and were earning positive returns; and (b) providing the Victim Investors bogus explanations for delayed and/or

incomplete dividend payments or redemptions. Victim Investors were also provided with back office online accounts associated with their investments at the website www.tradedeskfinancial.com (the "Tradedesk Website"). The Tradedesk Website allowed the Victim Investors to view their account balances and other information associated with their investment accounts similar to an online brokerage account.

11. At various times since in or around 2016, and particularly starting in or around 2018, the Victim Investors demanded the return of their funds. Schamens returned some Victim Investor funds, in part by using incoming funds from other Victim Investors in the manner of a Ponzi scheme. Since in or around 2018, however, Schamens has not returned all requested funds to Victim Investors who made withdrawal demands. Instead, Schamens has strung along the Victim Investors through misrepresentations and false promises.

12. To date, law enforcement has identified at least three confirmed victims of the scheme who have suffered collective losses of approximately \$3 million. Law enforcement has further identified approximately twelve additional individuals believed to be victims of the scheme based on a review of bank records associated with the Trading Groups.

Victim-1

13. According to information provided by Victim-1, Victim-1 was introduced to Schamens in or around 2014 by a mutual acquaintance. Victim-1 was looking for a brokerage firm to invest funds that Victim-1 recently withdrew from an IRA Victim-1 previously held at Charles Schwab. According to Victim-1, Schamens told Victim-

1 that Schamens operated an investment group that loaned money to day traders using funds derived from private investors. Schamens further told Victim-1 that the group generated its profits from service fees imposed on the traders and not the profitability of the trader who received the loan. Schamens represented to Victim-1 that an investment in the group would generate an estimated return of 1% monthly.

14. According to Victim-1, Schamens told Victim-1 that the funds used to finance the loans to the traders were controlled by one or more proprietary trading groups under Schamens' direction. Victim-1 identified TD and TFG as two of the Trading Groups that Victim-1 invested in through Schamens.

15. On or about September 24, 2014, Victim-1 made an initial investment with TD of approximately \$288,000, which represented the total value of Victim-1's IRA. According to Victim-1, Schamens instructed Victim-1 to first transfer the funds to Millennium. Once the funds were received by Millennium, Victim-1 instructed Millennium, at Schamens' direction, to invest the IRA funds with TD. The funds were then wired to the Tradedesk BOA Account. Between on or about January 30, 2015 and on or about January 5, 2018, Victim-1 made at least four additional investments in a similar manner (through both Millennium and Mainstar) with TD and/or TFG totaling approximately \$215,000 for a total investment of approximately \$503,000.

16. Victim-1 made similar investments in the Trading Groups on behalf of Victim-1's wife beginning on or about November 26, 2014 through on or about January 5, 2018. The total amount of these investments, which were also made through Millennium and Mainstar, was approximately \$275,000.

17. Finally, Victim-1 additionally made investments in the Trading Groups on behalf of Victim-1's company ("Company-1"). Specifically, between on or about March 30, 2015 and on or about August 21, 2018, Victim-1 made approximately eleven separate wire or bank transfers (one to the TD Bank Account and ten to the TFG Bank Account) totaling approximately \$2.5 million as investments with the Trading Groups.

18. Victim-1 further stated that in or around January 2016, Victim-1 made a redemption request for \$50,000 to determine the fund's degree of liquidity. The redemption was provided to Victim-1 in two separate wire transfers of approximately \$25,000 each in January 2016 and April 2016 respectively. Based on this investigation, the \$25,000 redemption payment made to Victim-1 in January 2016 came directly from another Victim Investor without his or her consent.

19. Over the life of the investments, Schamens provided Victim-1 with monthly account statements (the "Account Statements") for the investments made by Victim-1, Victim-1's wife, and Company-1 (the "Victim-1 Investments"). The Account Statements purported to show that the Victim-1 Investments were secure and were generating positive returns on a monthly basis. For example, in or around February 2018, Victim-1 received a monthly Account Statement for Victim-1's account with Tradedesk that covered the period from January 1, 2018 through January 31, 2018 (the "January 2018 Account Statement"). A review of the January 2018 Account Statement revealed that Victim-1's account with Tradedesk had generated a 1.76% return for the month of January 2018 and had grown approximately \$62,000 during

the month. Based on a review of bank records associated with the Trading Accounts, the Account Statements were fake and were provided to the Victim Investors by Schamens in order to provide them with the security that their investments were safe and generating consistent positive returns.

20. According to Victim-1, Victim-1 first suspected a problem with his investments in or around 2018 when he learned that another Victim Investor ("Victim-2") had difficulty withdrawing funds from his account with the Trading Groups. Shortly after learning about Victim-2's inability to withdraw funds, Victim-1 requested a \$500,000 redemption from Schamens on behalf of Company-1 to determine if there were any funds in the account.

21. Between March 14, 2019 and June 10, 2019, Victim-1 received a series of "redemption payments" from Schamens totaling \$350,000. Victim-1 stated that during this time, Schamens failed to provide him with certain documents, such as valuation sheets related to the investments, despite Victim-1's repeated requests. As a result, Victim-1 grew even more skeptical of Schamens, and, toward the end of 2019, advised Schamens that he wanted to withdraw the balance of all of his investments, including investments made on behalf of Victim-1's wife and Company-1, totaling approximately \$2.9 million. Shortly after making this request, Schamens received an approximately \$200,000 "redemption payment" from Schamens. To date, Victim-1 has not received any additional redemption payments.

22. According to Victim-1, Schamens promised that the funds would be returned to Victim-1 on a quarterly basis from a third-party affiliate called

Genihealth. This information was memorialized in a redemption notice provided to Victim-1 by Schamens in early 2020. According to the redemption notice, the value of Victim-1's investment accounts had grown substantially over the life of the respective investments. Specifically, according to the redemption notice, the value of Victim-1's investment account was approximately \$979,000, up from total investments of approximately \$504,000. Similarly, the purported value of Victim-1's wife's investment account was \$479,815.42 (up from total investments of approximately \$275,000), and the purported value of Company-1's investment account was \$3,780,613.11 (up from total investments of approximately \$2.5 million).

23. Following Victim-1's receipt of the redemption notice, he received no further redemption payments from Schamens. To date, Victim-1 has not received any additional redemption payments, despite his repeated requests to Schamens.

24. During this time, Victim-1 engaged in frequent communications with Schamens via text message and email in which Victim-1 demanded explanations for the delays in redemption payments. Schamens consistently made excuses for the delays and continued to falsely assure Victim-1 that wire transfers had been sent or were pending. For example, the following communications, among others, occurred between on or about March 6, 2020 and on or about June 10, 2020 regarding redemptions sought by Victim-1:

- a. On or about March 6, 2020, Victim-1 sent two text messages to Schamens that stated, in part, "My concern is now turning to payouts. How much for March 15...are we talking 500k roughly?" Schamens responded, "Yes."

- b. On or about March 10, 2020, Victim-1 sent a text message to Schamens that stated, "Hey can you confirm that I'm getting 500k on Friday." Schamens responded, in part, "Working on confirming Friday."
- c. On March 11, 2020, Victim-1 sent a text message to Schamens that stated, "Just looking for an answer. Am I going to see 500k in my acct Friday?" Schamens responded:

"Schedule goes out tonight. We had put down March 15 because that is the regular day for our processing after month end. If that day falls on Weekend we always go with next business day. These are large distributions that we have been planning on in conjunction with winding down the trading fund and winding up the HSA trading. We will make your distribution next week for sure but I am still trying for Friday. It may be we do part for Friday. I will have something definitely firm if we can do it Friday about 10PM. For now though I can't completely confirm the transfer will hit in time."

- d. On March 12, 2020, Victim-1 sent two text messages to Schamens that stated, "Dave am I safe to assume that I will get a 500 K wire from you on Monday" and, after receiving no response, "I will ask again. Haven't heard anything from you yet. Will I get a 500 K wire from you on Monday." Schamens responded, "Have not been with phone except during webinar. Will ping you ASAP in morning after I check in (sic) wire."
- e. On or about March 15, 2020, Victim-1 sent a text message to Schamens that stated, "I will assume you are still wiring me money tomorrow. You have told us and known and planned for this for months now." Schamens responded "...woke up yesterday with excruciating gout as a result of too much stress on ankle from moving all last week...Wire request was sent in Thursday. Ping you no later than 10AM on time." Victim-1 did not receive a wire on this date.
- f. On or about March 16, 2020, Schamens sent a text message to Victim-1 that stated, "No wire today due to doubling of house

margin and calls. We are restructuring trading and wire will go out this week....no one was prepared for this volatility." Victim-1 responded, "I knew you were gonna do this."

- g. Between March 17, 2020 and March 23, 2020, Victim-1 continued to exchange text messages with Schamens about the status of the redemption. On March 23, 2020, Schamens sent a text message to Victim-1 that stated that the expected wire would "post in AM."
- h. On or about March 24, 2020, Schamens sent a text message to Victim-1 that stated, "We are posting now. Ping you about 1030." No wire was received by Victim-1 on this date.
- i. On or about April 2, 2020, after still not receiving the promised redemption, Victim-1 sent a text message to Schamens that stated, "Where's my wire dave." Schamens responded, "I just saw you called. I did not have access to phone. Minor medical issue after webinar yesterday. Ping you ASAP with everything I promised 2 days ago."
- j. The following day, on April 3, 2020, Schamens sent Victim-1 a text message that stated, "So you will definitely have a wire next week. Sending you schedule by tomorrow morning. Trading account changes made. And more updates either late this evening or early AM. Quite honestly there has been a complete exhaustion on part of everyone from trying to complete workloads."
- k. On or about April 9, 2020, after still not receiving the promised redemption, Victim-1 sent Schamens a text message that stated, "Well I can safely assume I'm not getting a wire for monies I was promised months ago." Schamens responded, "Apologies for lack of response. Reconciliations will be done on April 15. Already did margin calculations based on current volume and lower prices. So enough capital to keep margin and payout will be available on April 16 for wire."
- l. On or about April 16, 2020, Victim-1 sent Schamens a text message that stated, "Dave it's Thursday and I have seen or heard nothing yet." Schamens responded, "We have a reporting site certificate issue late yesterday and today that was preventing accounting from doing updates. Resolved and Should show in an hour. This has slightly affected timing of wire." Victim-1 then asked, "So the wire of 500k will hit my account this afternoon?"

Schamens responded, "No. We are delayed. I will put out an email and also text by 6PM on new time."

- m. On or about April 17, 2020, Victim-1 sent Schamens two text messages that stated, "Ok still haven't heard from you and no wire. What is the problem today?" and "Dave what is going on. This is absolutely ridiculous and I am tired (sic) of these constant excuses. I told you I needed this over a month ago." Schamens did not respond and no wire was received by Victim-1 on this date.
- n. On or about May 20, 2020, after Victim-1 had still not received the requested redemption payment, Schamens sent an email to Victim-1 that stated, "per my call Friday, we were looking to send the wire either Monday or Tuesday this week, and I would confirm that Monday. I was not able to confirm either Monday or Tuesday. Today is Wednesday. No wire will be sent out today as our incoming wire has yet to post. I just confirmed we will have the incoming wire post tomorrow and will flip it to you asap."
- o. On or about May 26, 2020, Schamens sent another email to Victim-1 that stated, "per my text, this is to confirm we will now wire out funds that were due out on May 15, and instead wire out on June 1. We are delaying the wire due to delays at GeniHealth HSA algo accounts being opened at Interactive Brokers which replace the trading capital and keep the revenues the same level for Tradestream. This relationship was articulated in the Redemption notice. I can have a call about this if you like. Thanks."
- p. On or about June 4, 2020, Victim-1 received an email from Schamens regarding a \$200,000 redemption payment (despite Victim-1 having still not received the originally requested \$500,000 redemption). The email stated, in part, "...per the schedule you have and our phone conversation, we have requested and are processing a wire tomorrow in the amount of \$200,000 to [Company-1] from TFG Trading Fund, LLC. We will send you wire notification when the wire(s) go out." Victim-1 did not receive a wire on this date.

25. On or about June 10, 2020, Victim-1 received an email from an employee of Tradedesk that contained wire instructions for two wire transfers that were scheduled to be sent to Company-1 from TFG Trading on June 15, 2020 and

June 30, 2020 in the amounts of \$100,000 and \$200,000, respectively. The email attached two forms with details regarding the wires. A review of the forms revealed that the wires were scheduled to be sent on June 15, 2020 from an account held by TFG Trading at Chase Bank ending in 5525 (the "TFG Chase Account"). A review of the TFG Chase Account revealed that between January 2, 2020 and May of 2021, the TFG Chase Account never had a balance higher than \$42,044. In fact, on June 10, 2020, the date the above email was sent, the TFG Chase Account had a balance of \$1. On June 15, 2020, the date the wires were supposed to be sent, the TFG Chase Account had a balance of \$64. Based on a review of the TFG Chase Account, there is probable cause to believe that Schamens falsified the wire transfer forms sent to Victim-1 to provide Victim-1 with the false assurance that the wire transfers were forthcoming.

26. To date, Victim-1 has not received any additional redemption payments from Schamens or the Trading Groups related to the Victim-1 Investments.

Victim-2

27. According to Victim-2, he was introduced to Schamens in or around 2014 by Victim-1. Victim-2 stated that Victim-1 suggested that Victim-2 meet with Schamens after Victim-1 learned that Victim-2 had recently inherited money and was looking for a place to invest those funds.

28. Victim-2 stated that Victim-2 was told that Schamens operated an investment group that loaned money to day traders using funds derived from private investors. According to Victim-2, Schamens claimed that the group generated an

estimated rate of return of approximately 1% - 1.5% a month. Schamens further told Victim-1 that members of the investment group needed to have a million dollars of net assets and were required to make an initial investment of \$250,000 in the form of a "buy-in." Schamens told Victim-2 that Schamens was willing to waive the initial investment requirement and accept a lower "buy-in" from Victim-2 as a courtesy to Victim-2 for being a member of the law enforcement community.

29. On or about May 15, 2015, Victim-2 made an initial investment with Schamens of \$150,000. The funds were transferred to a bank account held by TD Trading ending in 6431.

30. Between on or about July 10, 2015 and on or about February 22, 2016, Victim-2 invested additional funds with TD and TFG totaling approximately \$255,000. Additionally, on or about June 30, 2016, Victim-2 transferred custody of an IRA with a value of approximately \$94,000 to Mainstar. At Schamens' direction, Victim-2 thereafter directed Mainstar to invest the funds in TFG and the funds were then wired to the TFG BOA Account.

31. According to Victim-2, in or around June of 2017 Victim-2 withdrew \$50,000 from his investment account. In or around October 2018, Victim-2 requested an additional \$70,000 redemption. Victim-2 ultimately received the redemption on or about January 23, 2019. However, according to Victim-2, Victim-2 had difficulty retrieving the funds and received a series of bad wires and a bounced check from Schamens during the time between the redemption request and the January 23 redemption.

32. According to Victim-2, on or about June 11, 2020, Victim-2 was also able to withdraw approximately \$13,000 from the funds transferred from Victim-2's IRA. Victim-2 stated that those funds were transferred by Schamens to a separate IRA account as a sign of good faith that a full redemption was forthcoming.

33. Similar to Victim-1, in early 2020, Victim-2 received a redemption schedule from Schamens. The document was almost identical to the redemption schedule provided to Victim-1 and indicated that Victim-2 would receive quarterly-redemption payments from Genihealth beginning on May 15, 2020 through May 15, 2021. The redemption schedule listed the purported value of Victim-2's individual investment as \$634,676.11 (up from an original investment of \$375,000). The redemption schedule further listed the value of Victim-2's IRA as \$201,311.02 (up from an original deposit of approximately \$94,000).

34. On or about July 7, 2020, Victim-2 received a final redemption payment of approximately \$41,969.00. To date, Victim-2 has not received any additional redemption payments from Schamens and has suffered total losses of approximately \$324,000. Similar to Victim-1, Victim-2 has also communicated with Schamens regarding the redemption payments and has received similar lulling emails and text messages as those described with Victim-1, above.

Financial Analysis

35. A review of bank records associated with the investments made by Victims-1 and -2 has revealed that the funds were not invested as promised by Schamens. Rather, the funds were largely used to: (a) finance Schamens' lifestyle;

(b) pay back prior victims in the manner of a Ponzi scheme; and (c) finance other expenditures unrelated to the investments made by the Victim Investors. For example:

Victim-1

July 15, 2016 (Victim-1 \$200,000 Investment)

36. On or about July 15, 2016, Victim-1 wired \$200,000 into the TFG BOA Account as an investment in TFG. At the time of the transfer, the TFG account had a balance of \$1.88. According to Bank of America records, Schamens was the only authorized signatory on the TFG BOA Account. Shortly after the funds entered the TFG BOA Account, \$200,000 was transferred from the TFG BOA Account to the Tradedesk BOA Account. As with the TFG BOA Account, Schamens is the only authorized signatory on the Tradedesk BOA Account. At the time of the transfer, the Tradedesk BOA Account had a balance of approximately \$33,000. A review of records associated with the Tradedesk BOA Account revealed that from on or about July 15, 2016 through on or about August 1, 2016, approximately \$231,000 was withdrawn from the Tradedesk BOA Account, resulting in a final balance of \$2,475.97. The following transactions were observed, among other transactions believed to have no affiliation with the investments of the Victim Investors:

- a. On or about July 15, 2016, \$140,000 was transferred from the Tradedesk BOA Account to an account held in the name of a law firm domiciled in Charlotte, North Carolina ("Law Firm-1"). According to its website, Law Firm-1 claims to specialize in divorce, elder law, and civil litigation.
- b. On or about July 21, 2016, an additional transfer in the amount of \$30,640 was sent from the Tradedesk BOA Account to a law

firm in Florham Park, New Jersey ("Law Firm-2"). Further investigation revealed that Law Firm-2 represented Schamens in a civil dispute involving a separate investment scheme.

- c. Further, from on or about July 15, 2016 through on or about July 26, 2016, \$37,000 was transferred from the Tradedesk BOA Account to a Bank of America account held in the name of Bold Analytics Ltd. dba TradeStream Analytics, Ltd (the "Bold Analytics BOA Account"). At the time of the transfer, the Bold Analytics BOA Account had a balance of \$2,175.29. Similar to the other depository accounts commonly used by Schamens, the Bold Analytics BOA Account identified Schamens as the only authorized signatory. Following the above transfers, on or about July 15, 2016, \$12,000 was wired from the Bold Analytics BOA Account to a foreign-based bank account purportedly controlled by an individual named Dmitry Filatov ("Filatov"). Later, on or about July 27, 2016, an additional \$13,399.77 was transferred to an entity identified as Equinix, Inc ("Equinix"). According to its website, Equinix is a real estate investment trust that invests in interconnected data centers. Based on this investigation, Victim-1 did not authorize his funds to be invested through Equinix.
- d. During the same time period, \$13,100 was transferred from the Bold Analytics BOA Account to a Bank of America account held by Schamens personally (the "Schamens BOA Account"). An analysis of the Schamens BOA revealed that a majority of the transactions conducted from the Schamens BOA Account appeared to be personal in nature.
- i. Finally, from on or about July 15, 2016 until July 26, 2016, approximately \$20,000 was collectively transferred from the Tradedesk BOA Account to four entities that regularly received bank transfers from the Tradedesk BOA Account while depositing little to no money into the account. These entities appeared to have no affiliation with the investments made by Victims-1 and -2.

August 5, 2016 (Victim-1 \$200,000 Investment)

37. On or about August 5, 2016, Victim-1 wired \$200,000 to the TFG BOA Account for an investment in TFG. At the time of the transfer, the TFG BOA Account had a negative balance of \$12.12. Shortly after the funds entered the

account, \$199,750 was transferred to the Tradedesk BOA Account. An analysis of the Tradedesk BOA Account revealed that from on or about August 5, 2016 through on or about August 15, 2016, approximately \$187,000 was withdrawn from the Tradedesk BOA Account. During that period, the Tradedesk BOA Account had a beginning balance of \$2,475.97 and an ending balance of \$15,041.07. The following transactions were observed, among other transfers believed to have no affiliation with the investments of the Victim Investors:

- a. On or about August 5, 2016, \$75,260 was transferred from the Tradedesk BOA Account to a Bank of America account in the name of Bull Bear Trading Partners, LLC (the "Bull Bear Account"). At the time of the initial transfer, the balance of the Bull Bear Account was \$57.01. Similar to the other business accounts, Schamens was identified as the only authorized signatory on the account.
- b. Soon thereafter, a wire transfer of \$50,235.01 was sent to an account held in the name an individual with the initials J.B. at Chase Bank (the "J.B. Transfer"). According to the corresponding wiring instructions, the purpose of the J.B. Transfer was to "close account." Based on this investigation, law enforcement believes J.B. is a potential victim of this scheme.
- c. Further, from on or about August 5, 2016 through on or about August 15, 2016, \$33,600 was transferred from the Tradedesk BOA Account to the Bold Analytics BOA Account. At the time of the initial transfer, the balance of the Bold Analytics Account was \$2,477.42. Soon thereafter, a total of \$20,000 was wired from the Bold Analytics BOA Account to foreign-based bank accounts separately controlled by Filatov and an individual named Vladimir Kaparkov ("Kaparkov"). During the same time period, \$11,250 was transferred from the Bold Analytics BOA Account to the Schamens BOA Account where it was used for apparent personal expenses.
- d. Further still, on or about August 8, 2016, \$55,000 was transferred from the Tradedesk BOA Account to a Bank of America account held in the name America Comes First Political

Action Committee (the “BOA PAC account”), which listed “David W Schamens (Treasurer)” as the only authorized signatory. When the funds entered the BOA PAC Account, the balance was \$0. Soon thereafter, a check in the amount of \$54,000 was issued from the BOA PAC Account to the Trump Victory Fund, a committee that raised money in part for Donald Trump’s 2016 presidential campaign.

June 8, 2017 (Victim-1 \$500,000 Investment)

38. On or about June 8, 2017, Victim-1 wired \$500,000 to the TFG BOA Account. At the time of the transfer, the TFG account had a balance of \$0.88. Shortly after the funds entered the account, \$499,975.00 was transferred from the TFG account to the Tradedesk BOA Account. From on or about June 8, 2017 through on or about August 4, 2017, approximately \$496,000 was withdrawn from the Tradedesk BOA Account. During that time period, the account had a beginning balance of \$356.36 and an ending balance of \$5,395.48. The following transactions were observed, among other transfers believed to have no affiliation with the investments of the Victim Investors:

- a. From on or about June 8, 2017 through on or about August 2, 2017, \$155,000 was transferred from the Tradedesk BOA Account to the Bold Analytics BOA Account. At the time of the initial transfer, the balance of the Bold Analytics BOA Account was \$91.35. On or about June 8, 2017, \$52,000 was wired from the Bold Analytics BOA Account to foreign-based bank accounts separately controlled by Kaparkov and Filatov, respectively. An additional \$9,000 was transferred to an entity identified as Webstone Inc., with no apparent affiliation with the Victim Investments. During the same time period, approximately \$82,500 was transferred from the Bold Analytics BOA Account to the Schamens BOA Account where the funds were used for apparent personal expenditures and political contributions.
- b. Further, from on or about June 16, 2017 through on or about July 10, 2017, \$200,125 was transferred from the Tradedesk

- BOA Account to the TD BOA Account. At the time of the initial transfer, the TD BOA Account had a negative balance of \$14.94. Soon thereafter, two bank transfers totaling \$50,000 were sent from the TD BOA Account to one or more accounts belonging to Victim-2. These transfers were the “redemption payments” received by Victim-1 discussed in Paragraph 31, above. Bank records further revealed that an additional \$150,000 was sent from the TD Trading Account to a foreign-based account controlled by an entity called Interactive Brokers.
- c. Further still, from on or about June 8, 2017 through on or about July 6, 2017, \$75,000 was transferred from the Tradedesk BOA Account to an entity believed to be a law firm (“Law Firm-3”) that previously represented one or more parties in a civil dispute involving Schamens. Further, on or about June 8, 2017, an additional \$25,000 was sent to account belonging to Law Firm-2.

June 1, 2018 (Victim-1 \$200,000 Investment)

39. On or about June 1, 2018, Victim-1 wired \$200,000 to the TFG BOA Account. At the time of the transfer, the TFG account had a balance of \$1. Shortly after the funds entered the account, \$200,000 was transferred from the TFG account to the Tradedesk BOA Account. From on or about June 1, 2018 through on or about June 21, 2018, approximately \$200,000 was withdrawn from the Tradedesk BOA Account. During that time period, the Tradedesk BOA Account had a beginning balance of \$1.55 and an ending balance of \$194.68. The following transactions were observed, among other transfers believed to have no affiliation with the investments of the Victim Investors:

- a. From on or about June 1, 2018 through on or about June 18, 2018, \$142,000 was transferred from the Tradedesk BOA Account to the Bold Analytics BOA Account. At the time of the initial transfer, the balance on the Bold Analytics BOA Account was \$5.48. Shortly thereafter, \$81,254.40 was wired from the Bold Analytics BOA Account to Equinix.

- b. During the same time period referenced above, \$6,000 was wired from the Bold Analytics BOA Account to a foreign-based bank account purportedly controlled by Filatov and approximately \$49,500.00 was transferred to the Schamens BOA Account where it was used for apparent personal expenditures.
- c. On or about June 1, 2018, \$15,000 was sent from the Tradedesk BOA Account to an account belonging to Law Firm-2.
- d. From on or about June 4, 2018 through on or about June 21, 2018, approximately \$10,000 was debited from the Tradedesk BOA Account. The debits were derived from purchases made using a check card linked to the account.

Victim-2

June 30, 2016 (Victim-2 \$94,168.87 Investment)

40. As set forth above, on or about June 30, 2016, Victim-2 caused \$94,168.87 from a previously held IRA to be transferred to Mainstar at the direction of Schamens. Shortly thereafter, also at the direction of Schamens, Victim-2 directed Mainstar to transfer the funds to the TFG BOA Account as an investment in TFG. At the time of the transfer, the TFG BOA Account had a balance of \$2.01. Shortly after the funds entered the account, \$94,135.00 was transferred from the TFG BOA Account to the Tradedesk BOA Account. From on or about June 30, 2016 until July 8, 2016, approximately \$100,000.00 was withdrawn from the Tradedesk BOA Account. During that time period, the Tradedesk BOA Account had a beginning balance of \$245.45 and an ending balance of \$4.68. The following transactions were observed, among other transfers believed to have no affiliation with the investments of the Victim Investors:

- a. From on or about June 30, 2016 through on or about July 5, 2016, \$73,100 was transferred from the Tradedesk BOA Account to the

Bold Analytics BOA Account. At the time of the initial transfer, the balance on the Bold Analytics BOA Account was \$0.67. Shortly thereafter, a total of \$26,000 was wired from the Bold Analytics BOA Account to foreign-based bank accounts separately controlled by Filatov and Kaparkov. During approximately the same period, \$22,015.00 was transferred from the Bold Analytics BOA Account to the Schamens BOA Account, where the funds were used for apparent personal expenditures.

- b. Further, on or about June 30, 2016, \$3,800.00 was wired out of the Tradedesk BOA Account and into an account that purportedly belonged to an individual named Christopher Doubek ("Doubek"). During the course of the investigation, law enforcement obtained multiple subscription agreements which identified "Christopher R. Doubek" as a managing member of TFG. The agreements were purportedly sent to Mainstar from the email address dschamens@tradestreamanalytics.com for the purpose of memorializing the purchase of stock from TFG by Victims-1 and -2.
- c. Further still, from on or about July 1, 2016 through on or about July 8, 2016, approximately \$6,000 was debited from the Tradedesk BOA Account. The debits were derived from purchases made using a check card linked to the Tradedesk BOA Account and had no apparent connection to the investments made by the Victim Investors.

The SUBJECT PREMISES/SCHAMENS

41. Schamens currently resides at the **SUBJECT PREMISES** and has since in or around December 2019.

42. According to information provided by Web.com, the Tradedesk Website is associated with a Web.com account that lists Schamens as the primary account holder. As the primary account holder, Schamens is permitted to perform all actions on the account and the products and services associated with that account, to include initiating and revoking permissions of other users. According to Web.com records, the mailing address associated with the account is the **SUBJECT PREMISES**.

43. Further, based on this investigation, at least two different Chase bank accounts used by Schamens in furtherance of the scheme described herein list Schamens as the signatory and the **SUBJECT PREMISES** as the mailing address associated with the accounts. Based on this investigation, Schamens used at least one of the accounts to fund a different account at Chase that was used to send at least one fraudulent "redemption payment" to Victim-1.

44. Additionally, based on this investigation, at least one of the email accounts used by Schamens to communicate with the Victim Investors (the "Schamens Email Account") is hosted by Microsoft. According to records provided by Microsoft, the Schamens Email Account was accessed from an IP Address ending in 48 (the "48 IP Address") at various times between December 25, 2020 and February 5, 2021. The investigation revealed that the 48 IP Address resolves to an account at Northern State Cable/Internet ("Northern State"). According to records provided by Northern State, the 48 IP Address is assigned to an account subscribed to by Schamens at the **SUBJECT PREMISES**.

45. Finally, based on my training, experience, and participation in this and many other fraud investigations, as well as my conversations with other agents and officers involved in this and other such investigations, I believe the following:

- a. Individuals involved in the type of scheme described above must keep evidence of their schemes, such as contact information for victims of the scheme, and lists of identities and accounts used in the scheme, simply to keep the scheme going. These individuals often use the proceeds of their fraud to purchase expensive items, or keep the proceeds in the form of cash to make their crime harder to detect.

- b. More sophisticated criminals often store their illicit proceeds in digital currency or on prepaid credit cards, again to make the proceeds hard to trace. Typically, they maintain all this evidence where it is close at hand and safe, such as in their residences, vehicles, and digital devices, which are also commonly stored in their residences and vehicles.
- c. Such individuals commonly use cellular telephones to compartmentalize their contacts, and communicate with their victims by phone, email, and text messages. I know that individuals who commit crimes with the aid of electronic devices do not readily discard them, as computers, tablets and cell phones are expensive items that are typically used for years before being upgraded or discarded. I further know that when individuals obtain new cellular telephones and other devices that they will often back up information from their previous device or devices to the new device. As set forth herein, Schamens has used both text messaging and email to communicate with the Victim Investors. At set forth above, Schamens accessed at least one of the email accounts used to communicate with the Victim Investors from the **SUBJECT PREMISES** as recently as February 2021, the date of the Government's request for records.

46. Based on the foregoing, there is probable cause to believe that Schamens who resides at the **SUBJECT PREMISES**, has engaged in the Specified Federal Offenses. There is further probable cause to believe that evidence of the Specified Federal Offenses will be located within the **SUBJECT PREMISES** including, but not limited to, electronic devices used by Schamens in furtherance of the scheme as well as bank records and other documentary evidence, including the identities of additional victims of the scheme. There is further probable cause to believe that such evidence will be found on Schamens' person, including, but not limited to, cellular telephones and other electronic devices.

**COMPUTERS, ELECTRONIC STORAGE,
AND FORENSIC ANALYSIS**

47. As described above and in Attachment B, this application seeks permission to search for records that might be found on the **SUBJECT PREMISES**, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all pursuant to Rule 41(e)(2)(B).

48. *Probable cause.* I submit that if a computer or storage medium is found on the **SUBJECT PREMISES**, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In

addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

49. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the **SUBJECT PREMISES** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that

show what tasks and processes were recently active. Web browsers, E-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or

storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the

computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain unauthorized access to a victim computer, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence

of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

50. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the **SUBJECT PREMISES**, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on the **SUBJECT PREMISES** could be unreasonable. As explained above, because the

warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the **SUBJECT PREMISES**. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

51. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques,

including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

BIOMETRIC ACCESS TO DEVICES

52. Based on my training and experience, and the investigation to date, I believe that it is possible that the **SUBJECT PREMISES** will contain at least one smart device, such as an iPhone or Android device.

53. I know from my training and experience, as well as from information found in publicly available materials, that Apple Inc. ("Apple"), Sony, Motorola, and Samsung, among other companies, produce devices (such as phones and tablets) that can be unlocked through biometric features in lieu of a numeric or alphanumeric passcode. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and, for some devices, the users can select which features they would like to utilize.

54. If a device is equipped with a fingerprint scanner, once a user has set up the fingerprint sensor feature in the security settings of the device, the user can unlock the device by placing any of the registered fingerprints or thumbs (an individual can register up to 5 fingerprints that can be used to unlock a device) on the device's fingerprint sensor. If that sensor recognizes the fingerprint, the device unlocks. Most devices can be set up to recognize multiple prints, so that different prints, not necessarily from the same person, will unlock the device.

55. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Similarly, Face ID allows a user to unlock the iPhone X. It provides intuitive and secure authentication enabled by the TrueDepth camera system, which uses advanced technologies to accurately map the geometry of the user's face. Face ID confirms attention by detecting the direction of the user's gaze, then uses neural networks for matching and anti-spoofing so the user can unlock the phone with a glance. Face ID automatically adapts to changes in the user's appearance, and carefully safeguards the privacy and security of the user's biometric data. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face and Face ID.

56. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises.

The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

57. In my training and experience, users of devices with a biometric sensor features often enable them because it is considered to be a more convenient way to unlock the device than by entering a numeric or alphanumeric passcode or password, as well as a more secure way to protect the device's contents. This is particularly true when the user of the device is engaged in criminal activities and thus have a heightened concern about securing the contents of the device.

58. The passcode or password that would unlock a smartphone device at the **SUBJECT PREMISES** are not known to law enforcement. Thus, it will likely be necessary to apply biometrics on any biometric sensor-enabled devices which fall within the scope of the warrants in an attempt to unlock the devices for the purpose of executing the search authorized by this warrant. Attempting to unlock the relevant devices with the use of biometrics is necessary because the agents may not otherwise be able to access the data contained on those devices for the purpose of executing the searches authorized by this warrant.

59. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. Thus,

in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

60. Although I do not know which of a given user's 10 fingerprints is capable of unlocking a particular device, based on my training and experience I know that it is common for a user to unlock a fingerprint sensor-enabled device via the fingerprints on thumbs or index fingers. In the event that law enforcement is unable to unlock any devices as described above, successive failed attempts will simply result in the device requiring the entry of a password or passcode before it can be unlocked.

61. Due to the foregoing, I request that the Court authorize law enforcement to unlock the smart devices, such as iPhones, found at the **SUBJECT PREMISES** using one of the aforementioned biometric features. Specifically, the warrant permits law enforcement personnel to take reasonable measures to do the following: obtain from Schamens, or a resident any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any smart device, including to (1) press or swipe the fingers (including thumbs) to the fingerprint scanner of a device(s) found at the **SUBJECT PREMISES**; (2) hold a device(s) found at the **SUBJECT PREMISES** in front of Schamens, or a resident while instructing him/her to remain still with his/her eyes looking forward to activate the facial recognition feature; and/or (3) hold a device(s) found at the **SUBJECT PREMISES** in front of the face of Schamens, or a resident to activate the iris

recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.

CONCLUSION

62. I submit that this affidavit supports probable cause for a warrant to search the **SUBJECT PREMISES**, described in Attachment A-1 and the person of Schamens, described in Attachment A-2, and seize the items described in Attachment B.

Respectfully submitted,

/s/James Gallo

James Gallo
Special Agent, HSI

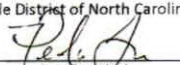
On this day, the applicant appeared before me by reliable electronic means, that is by telephone, was placed under oath, and attested to the contents of this Application for a search warrant in accordance with the requirements of Fed. R. Crim. P. 4.1.



8/27/2021 8:48 a.m.

Hon. Joe L. Webster
United States Magistrate Judge



Certified to be a true and
correct copy of the original.
John S. Brubaker, Clerk
U.S. District Court
Middle District of North Carolina
By: 
Deputy Clerk
Date: August 27, 2021

ATTACHMENT A-1

Property to be searched

The property to be searched is **812 Northern Shores Point Greensboro, North Carolina, 27455**, further described as a single-family, multiple-story, residence with stucco siding and a stone turret entryway. The main entrance is in the center of the house and is surrounded by trees and two rows of small bushes. The windows on the first floor have dark colored shutters, while the windows on the second floor do not have shutters. A circular driveway is located in front of the residence along with a decorative fountain. The residence is within the Northern Shores Estates subdivision, which is a gated community. A photograph of the **SUBJECT PREMISES** is below:



ATTACHMENT A-2
PERSON TO BE SEARCHED

David W. SCHAMENS, including any items that he is possessing and/or controlling at the time of the execution of the warrant. This includes items in SCHAMENS' pockets or hands (like digital devices or briefcases) or on SCHAMENS' back (like a backpack) at the time of the execution of the warrant. SCHAMENS resides at the **SUBJECT PREMISES** and has a date of birth of 07/16/1957. A photo of SCHAMENS is below:



ATTACHMENT B

Property to be seized

1. All records relating to a violation of 18 U.S.C. § 1343 (wire fraud), 18 U.S.C. § 1344 (bank fraud), 18 U.S.C. § 1956 (money laundering), 18 U.S.C. § 1957 (transacting in criminal proceeds), and 15 U.S.C. §§ 78j(b) and 78ff, and 17 C.F.R. § 240.10b-5 (securities fraud) (the “Specified Federal Offenses”), specifically:

- a. Records relating to the operation, control, and/or use of the name of the following businesses: TradeStream Analytics, TD Trading, TFG Trading, Tradedesk Financial, and Genihealth;
- b. Records relating to any business operated by David Schamens (“Schamens”);
- c. Bank statements, bank checks, cash receipts, money transfer records and receipts, money remittance instructions, customer information and records, sales records, ledgers showing cash and checks received, contracts, fax records, correspondence, including but not limited to correspondence with others regarding the transmission of money, printed emails, letters, faxes, and telephone logs or messages that constitute evidence of money laundering;
- d. Address and/or telephone books, Rolodex indices, invoices, communications, and any papers or records reflecting names, addresses, email addresses, telephone numbers, pager numbers, facsimile numbers

and/or telex numbers of co-conspirators, financial institutions, and other individuals or businesses with whom a financial relationship exists;

e. Books, records, invoices, receipts, records of real estate transactions, bank statements and related records, passbooks, money drafts, letters of credit, money orders, bank drafts, cashier's checks, bank checks, safe deposit box keys, money wrappers, and other items evidencing the obtaining, secreting, transfer, and/or concealment of assets and the obtaining, secreting, transfer, concealment and/or expenditure of money;

f. United States currency, digital currency such as Bitcoins stored on electronic wallets or other means, and records relating to income derived from the Specified Federal Offenses and expenditures of money and wealth, for example, money orders, wire transfers, cashier's checks and receipts, passbooks, checkbooks, check registers, securities, precious metals, jewelry, antique or modern automobiles, including stocks or bonds in amounts indicative of the proceeds of the Specified Federal Offenses;

g. Cellular telephones (including searching the memory thereof) and used to generate, transfer, count, record and/or store the information and evidence described in this Attachment, including cellular telephones on Schamens' person;

h. Photographs, records, and documents, including still photographs, negatives, video tapes, films, undeveloped film and the contents therein, slides, and any video, recording or photographic equipment containing the

aforementioned items, containing information regarding the identities of victims, coconspirators, or others involved in the Specified Federal Offenses;

- i. Indicia of occupancy, residency, ownership and/or use of the **SUBJECT PREMISES**, including but not limited to, utility and telephone bills; canceled envelopes; rental, purchase or lease agreements; and keys
- j. Articles of Incorporation, corporate resolutions, corporate minute books, corporate stock books, corporate stock certificates, corporate state charters, records of corporate franchise taxes paid, corporate financial statements, profit and loss statements, balance sheets, and statements of cash flow;
- k. General journals, cash receipt journals, cash disbursement journals, sales journals and computer printout sheets;
- l. General ledgers and subsidiary ledgers including notes receivables, accounts receivables, accounts payable, notes payable, adjusting journals and closing ledgers;
- m. Receipts and invoices for all expenditures;
- n. All Federal income tax returns, Forms 1040, W-2, 1099, 1120, 940, 941, K-1 , or copies of same and supporting work papers, summary sheets, and analyses used in the preparation of the tax returns
- o. Records regarding trading and/or transacting in any kind of security;
- p. Records relating to the solicitation, contracting, negotiating, or closing of any investment agreement;

q. Records of payments made in connection with the Specified Federal Offenses;

r. All personal financial statements, contact bids, proposals, closing statements, warranty deeds of trust, release deeds, or other documentation supporting conveyances and/or ownership of properties, and vehicle registration and titles; and

s. Safes, key-lock strong boxes, suitcases, locked cabinets, and other types of locked or closed containers used to secrete and store currency, books, records, documents, financial instruments, and other items of the sort described above. Law enforcement officers executing this Warrant are specifically authorized to open any such locked safes or containers including, where necessary, by using force.

2. Computers or storage media used as a means to commit the violations described above, including computers or storage media found on Schamens' person.

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of the use, ownership, access, or control of the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames

and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, correspondence, cookies, records of user-typed web addresses and search terms, and caches;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software through forensic artifacts found on device described herein;

d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. passwords, encryption keys, handwritten records referencing or revealing instructions to access the COMPUTER, and other access devices that may be necessary to access the COMPUTER;

g. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER; and

h. records of or information about Internet Protocol addresses used by the COMPUTER.

4. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

During the execution of the search of the **SUBJECT PREMISES** described in Attachment A, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the **SUBJECT PREMISES** and reasonably believed by law enforcement to be a user of a device found at the premises, to the fingerprint scanner of the device; (2) hold a device found at the premises in front of the face those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

Prior to the execution of the search, the government will establish a search filter team (the "Search Filter Team"). The Search Filter Team will include an attorney for the government. Members of the Search Filter Team will not include any attorney, agent, paralegal, or other person who is investigating or prosecuting the case (otherwise known as the "Prosecution Team"). Only members of the Search Filter Team will execute the search of the **SUBJECT PREMISES**. Members of the Prosecution Team may be present at the search location but only for such purposes as (1) providing information about the investigation to the Search Filter Team to assist the Search Filter Team's determination of what to seize, or (2) interviewing a target or other person. At the time the warrant is executed, the only review of evidence that will occur will be conducted by the Search Filter Team and is limited to the review that is required to determine whether evidence is within the scope of the warrant.

Once the search is complete, the Search Filter Team will provide the collected electronic and paper materials to a member of the government's technical support staff to scan into a document review system. Without reviewing the seized materials, the Prosecution Team will develop search terms to run against the seized materials to segregate materials that are potentially attorney-client privileged or subject to the work product doctrine ("Potentially Protected Materials"). The Search Filter Team will add further terms based on their search of the Subject Premises. The Search Filter Team will not share these additional terms with the Prosecution Team.

The Search Filter Team will apply the search terms to the collected materials, and it will segregate documents which contain any search term hit as Potentially Protected Materials. The Filter Team may not describe the contents or substance of any Potentially Protected Materials to the Prosecution Team. The Filter Team will provide all materials that are not Potentially Protected Materials to the Prosecution Team.

After beginning to review the non-segregated materials, if the Prosecution Team identifies additional Potentially Protected Materials, the Prosecution Team will discontinue review until a Filter Team of government attorneys and agents is established. Members of the Search Filter Team may serve on the Filter Team. The Filter team will include an attorney for the government. The Filter Team will not include members of the Prosecution Team. The Filter Team will have no future involvement in the investigation of this matter.

The Filter Team will review the seized communications and segregate Potentially Protected Materials (e.g., communications that are to/from an attorney, or that otherwise reference or reflect attorney advice. At no time will the Filter Team advise the Prosecution Team of the substance of any of the Potentially Protected Materials. Based on that review, if the Filter Team concludes that any of the Potentially Protected Materials are not protected (e.g., the communication includes a third party or the crime-fraud exception applies), the Filter Team may designate those materials as Post-Filter Nonprotected Materials. The Filter Team will not provide Potentially Privileged Materials or Post-Filter Nonprotected Materials to the Prosecution Team without either obtaining (1) an agreement from defense counsel/counsel for the potential privilege holder, or (2) a court order.

This investigation is presently covert, and the government believes that the subject of the search is not aware of this warrant.